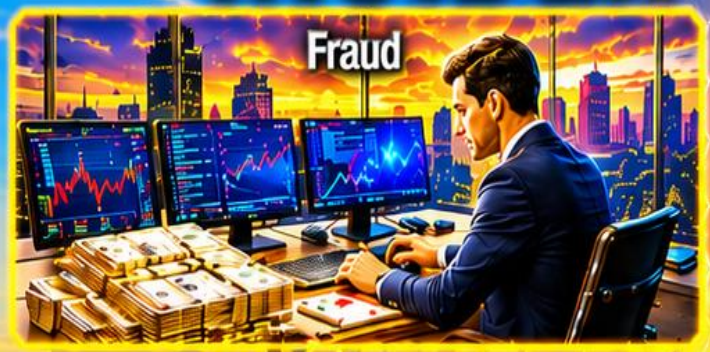
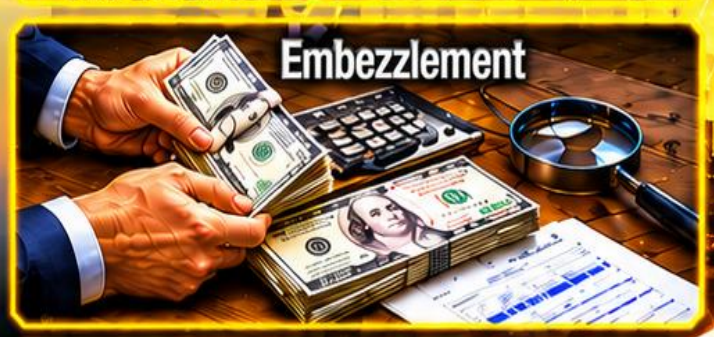
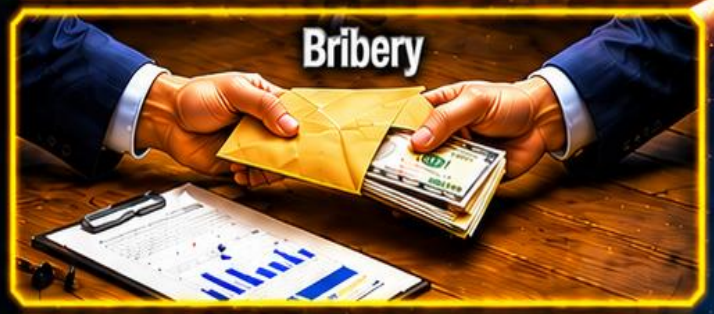
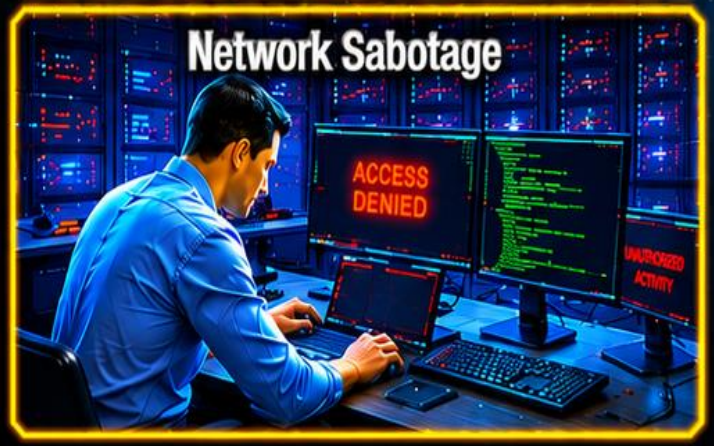
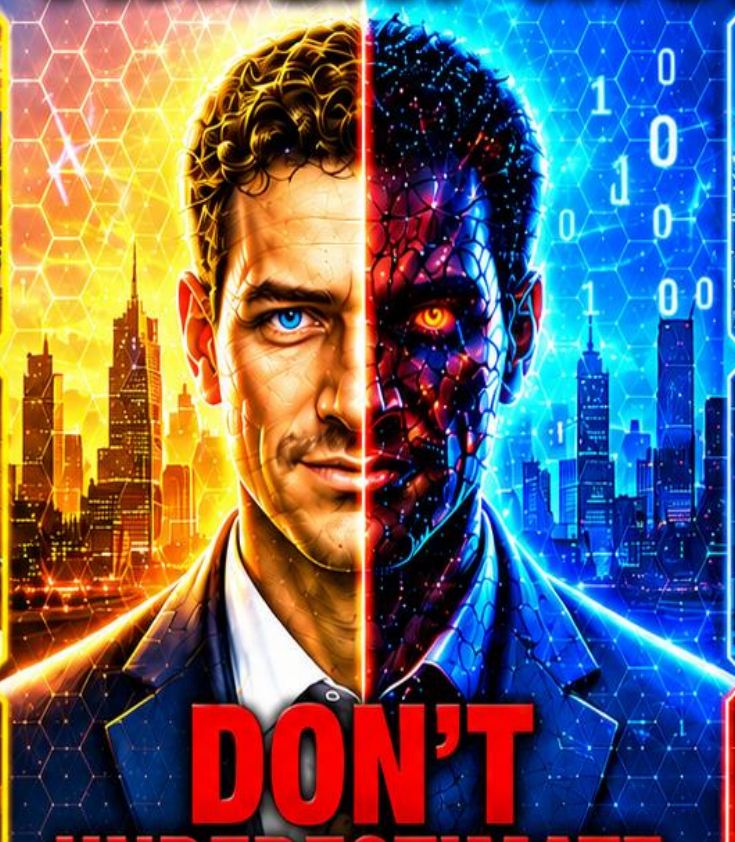
INSIDER THREAT INCIDENTS







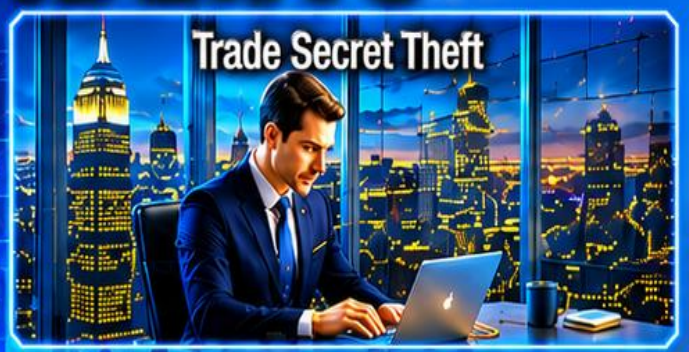


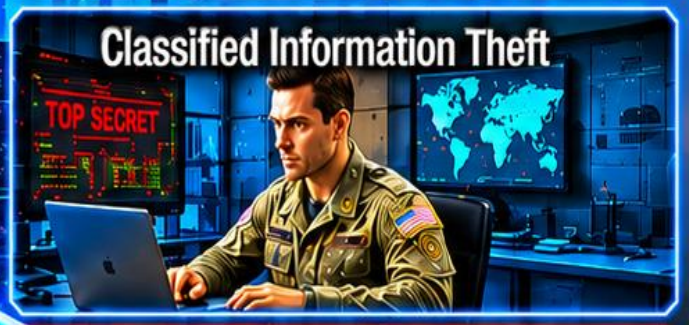


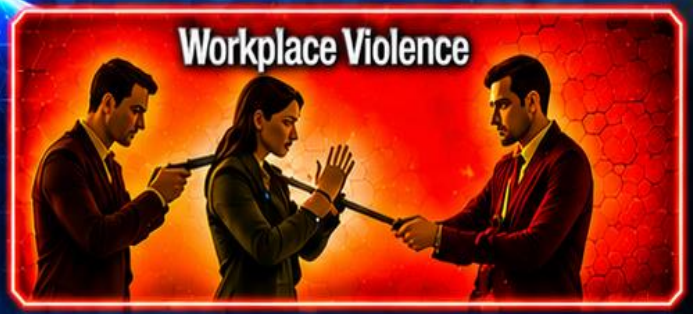
DON'T UNDERESTIMATE THE CAPABILITIES OF THE HUMAN OPERATING SYSTEM

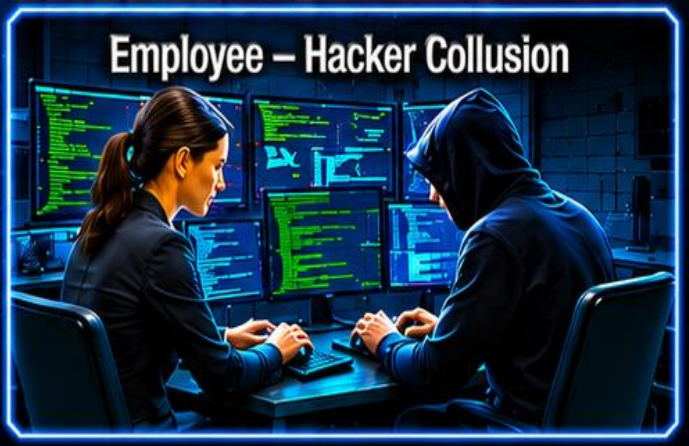
Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group









BUSINESS SURVIVABILITY - COULD YOUR JOB BE AT RISK?

The purpose of this report is to raise awareness of the Insider Threat problem. Some organizations may brief their employees on the Insider Threat problem and the importance of reporting employees that could harm the organization in many different ways.

But some organizations may only provide basic or limited examples of Insider Threat incidents. This may cause some employees to just brush off the Insider Threat problem and the importance of reporting employees. The severe financial damages and other operational impacts from an Insider Threat incidents are outlined in this report.

What if you were told you could lose your job because of a co-worker. Would you reconsider reporting an employee? Or would you reconsider taking harmful actions against your employer that were violations of security policies, or criminal actions that might cause you to loose your job and face criminal charges and legal expenses?

Insider Threats are also a business survivability problem. **Companies have had large layoffs or gone out of business because of the malicious actions of employees, as referenced on page 15.** The purpose of an Insider Risk Management Program is to identify problems with employees, so severe financial damages and other damaging impacts are avoided.

BACKGROUND & INFORMATION PRESENTED IN THIS DOCUMENT

The National Insider Threat Special Interest Group (NITSIG) was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center (ISAC), as no such ISAC existed. The comprehensive reports and guidance provided by the NITSIG, quickly fueled its memberships growth to become the largest U.S. / Global Insider Risk Management ISAC.

The NITSIG in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for **15+** years. This research has evaluated and analyzed over **7,400**+ Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

Download Monthly & Specialized Insider Threat Incident Reports
www.insiderthreatincidents.com

If you are interested in receiving the Insider Threat Incidents Reports via email, please send your request to:
jimhenderson@nationalinsiderthreatsig.org

WHO CAN BE AN INSIDER THREAT?

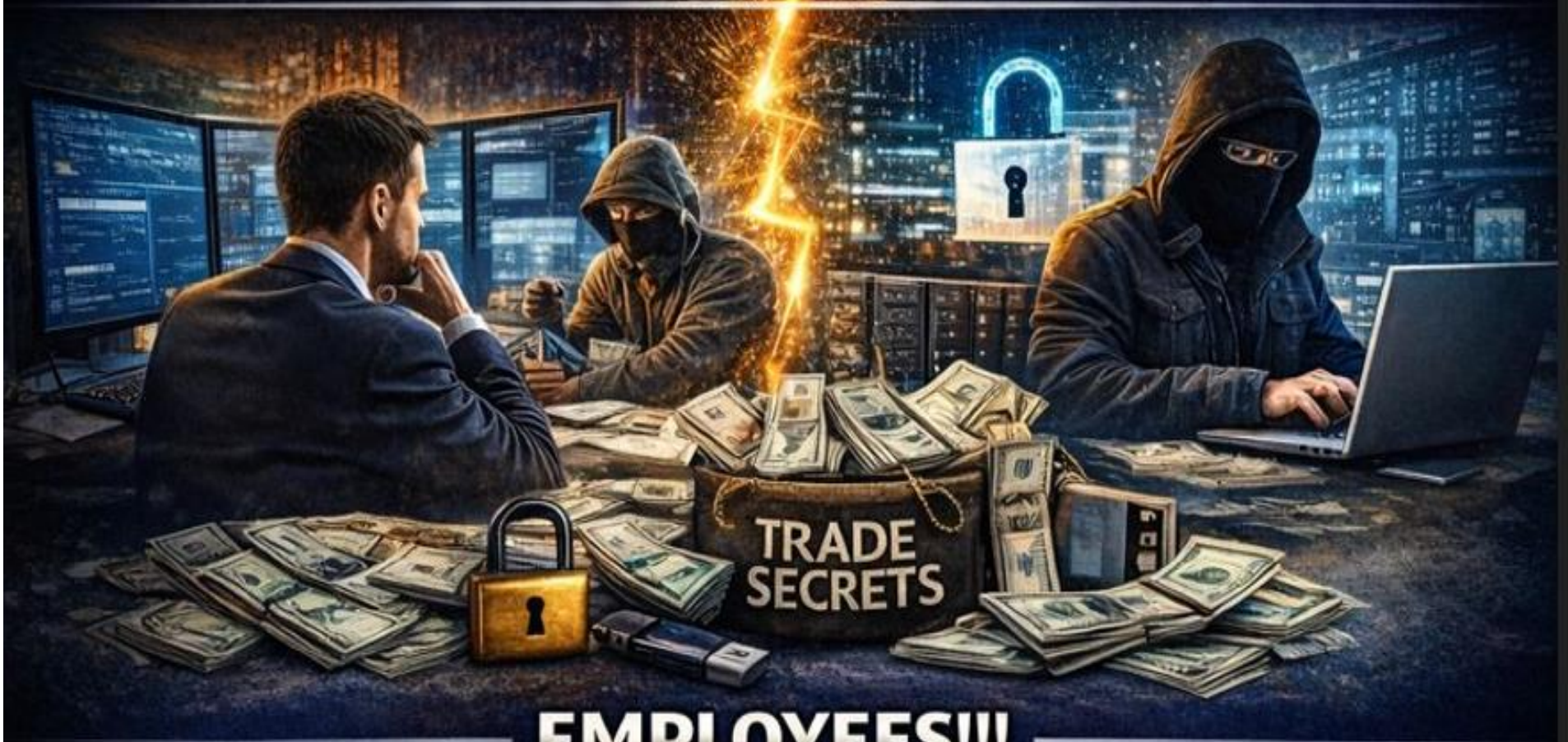
INSIDER THREAT (Simplistic)

Insider Threat - The potential for an individual (Employee) who has or had authorized access to an organization's critical assets (Facilities, Financial Assets, Employees, Data, Computer Systems - Networks) to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

INSIDER THREAT (Expanded)

- ☐ Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- ☐ Current & Former Employees / Contractors - Trusted Business Partners
- ☐ Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- ☐ Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry, Etc.)
- ☐ Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- ☐ Negligent Employees - Knows Security Policies & Procedures, But Disregards Them. Intentions Are Not Malicious.
- ☐ Opportunist Employees - Someone Who Focuses On Their Own Self Interests. Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.
- ☐ Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Their Goals (Micro Managed, Etc.)
- ☐ Employee Fraud - Embezzlement, Contracting & Kickbacks, Payroll / Time & Attendance, Expense Reports, Etc.
- ☐ Collusion By Multiple Employees To Achieve Malicious Objectives
- ☐ Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- ☐ Employees Involved In Foreign Nation State Sponsored Activities (Recruited – Incentives To Steal From Employer)
- ☐ Employees Using AI Systems In A Manner That Violates The Organizations AI Acceptable Use Policy
- ☐ Employees Threatening Or Involved In Workplace Violence, Bullying, Etc.

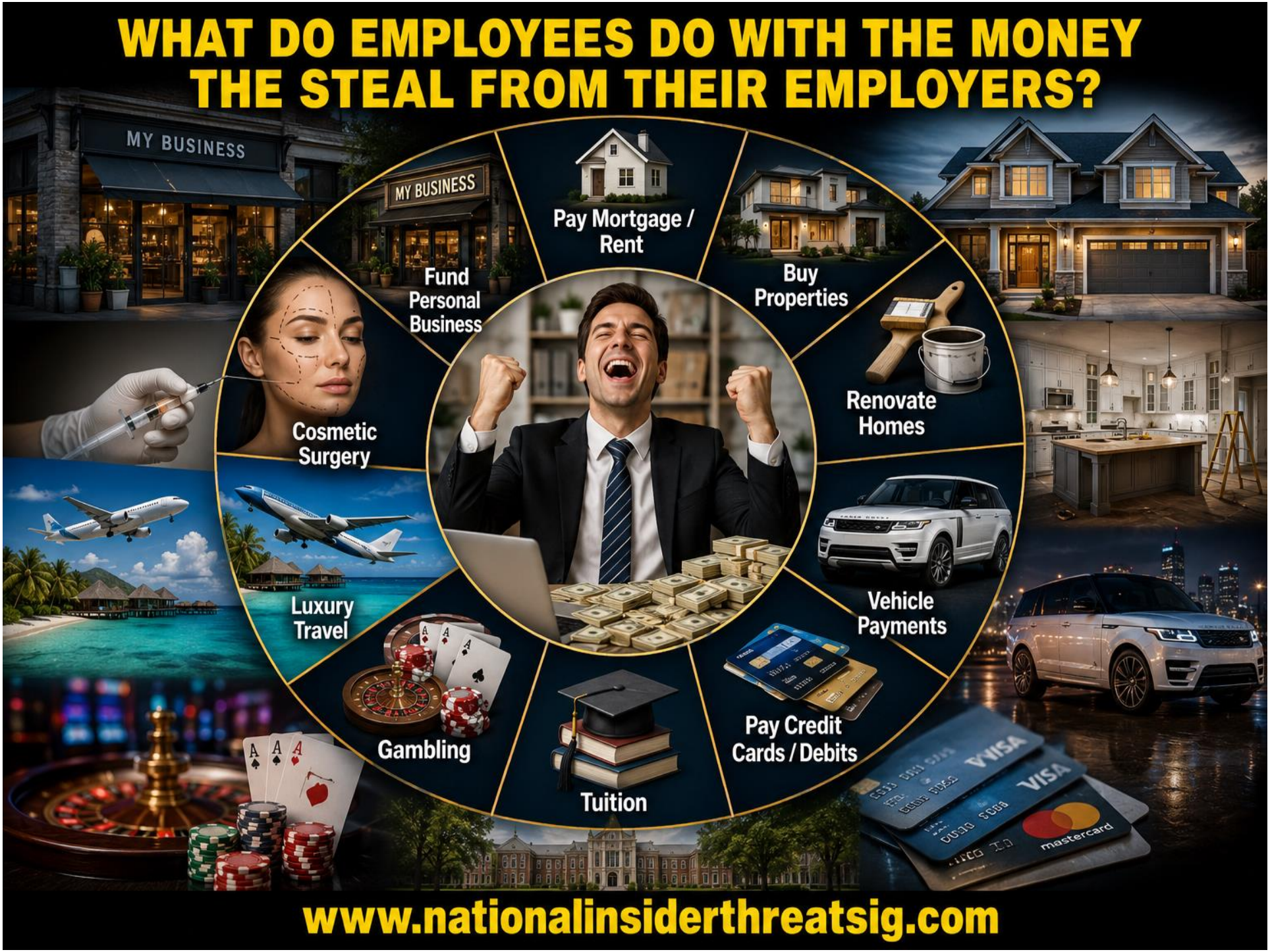
INSIDER THREATS vs HACKERS:
WHO CAUSES MORE DAMAGE?



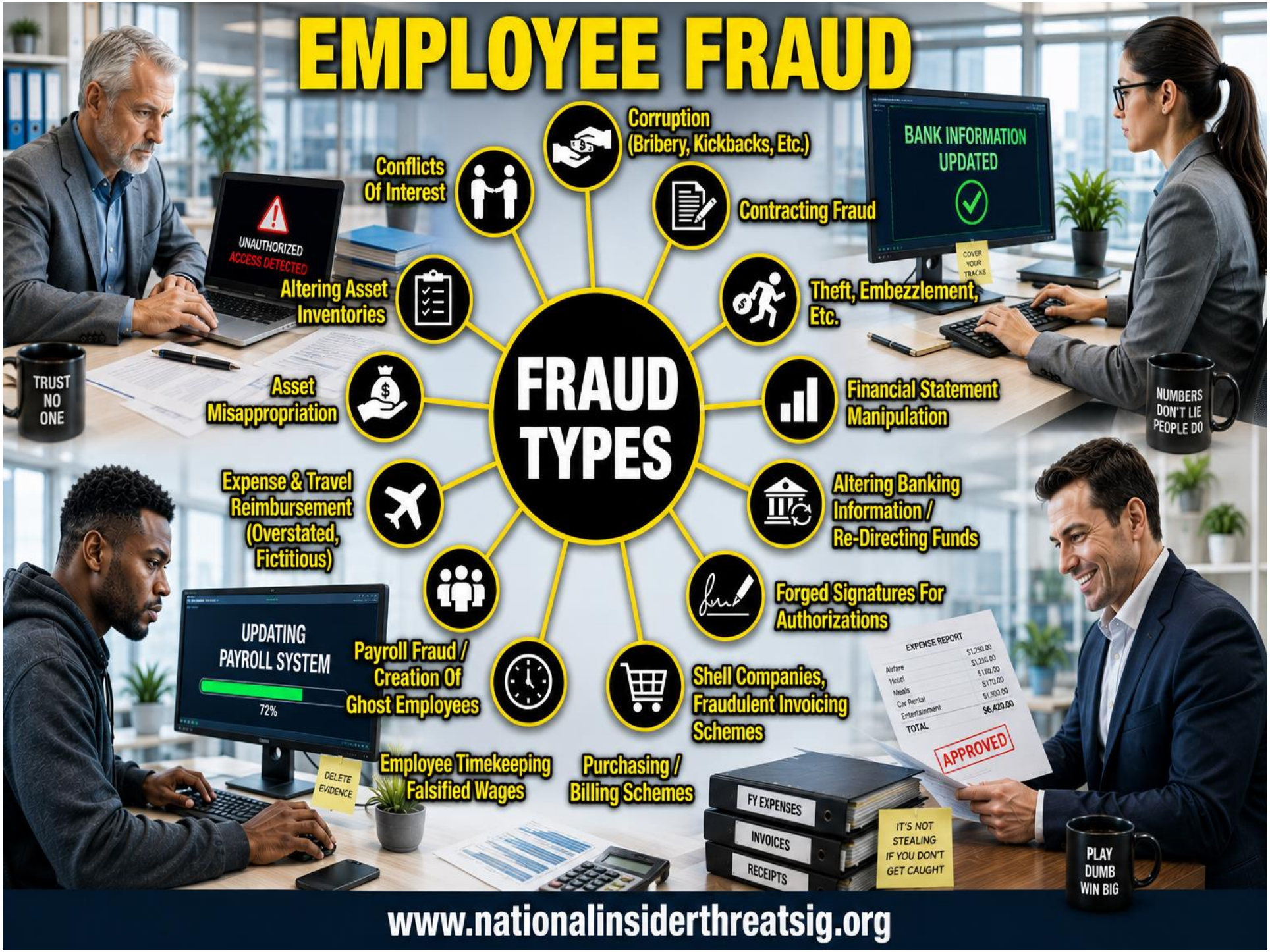
EMPLOYEES!!!

The most damaging security incidents are not just caused by information technology security vulnerabllities, hackers or ransomware. They are caused by malicious employees who are disgruntled and have personal grievances against their employers.

WHAT DO EMPLOYEES DO WITH THE MONEY THE STEAL FROM THEIR EMPLOYERS?



www.nationalinsiderthreatsig.com


EMPLOYEE FRAUD
FRAUD TYPES
Corruption (Bribery, Kickbacks, Etc.)
Conflicts Of Interest
Contracting Fraud
Altering Asset Inventories
Theft, Embezzlement, Etc.
Asset Misappropriation
Financial Statement Manipulation
Expense & Travel Reimbursement (Overstated, Fictitious)
Altering Banking Information / Re-Directing Funds
Forged Signatures For Authorizations
Payroll Fraud / Creation Of Ghost Employees
Shell Companies, Fraudulent Invoicing Schemes
Employee Timekeeping Falsified Wages
Purchasing / Billing Schemes
UNAUTHORIZED ACCESS DETECTED
TRUST NO ONE
BANK INFORMATION UPDATED
COVER YOUR TRACKS
NUMBERS DON'T LIE PEOPLE DO
UPDATING PAYROLL SYSTEM
72%
DELETE EVIDENCE
EXPENSE REPORT
Airfare $1,250.00
Hotel $1,230.00
Meals $780.00
Car Rental $770.00
Entertainment $1,500.00
TOTAL $6,420.00
APPROVED
FY EXPENSES
INVOICES
RECEIPTS
IT'S NOT STEALING IF YOU DON'T GET CAUGHT
PLAY DUMB WIN BIG
www.nationalinsiderthreatsig.org

INSIDER THREAT INCIDENTS REPORT FOR JANUARY 2026

EXAMPLES FROM REPORT / (STP = Sentenced To Prison)

- Check Point Software Research Reveals State Sponsored Hackers Are Recruiting Employees From Major Companies With Financial Incentives Ranging From $3,000 - $15,000

- U.S. Navy Sailor STP For Spying For China

- Employee Working For U.S. Small Business Administration & Internal Revenue Service Charged For Role In Stealing $3.5 Million+

- U.S. Government Congressional Employee Charged For Theft Of 240 Cell Phones Valued At $150,000+ / Sold To Pawn Shop

- Company Employee STP For Stealing $28 Million By Creating Fake Company And Diverting Funds

- TD Bank Employee Pleads Guilty To Accepting Bribes For Facilitating $26 Million+ Colombian ATM Money Laundering Scheme

- 4 Amtrak Employees Admit Participating In $11 Million Health Care Fraud / Kickback Scheme

- Aviation Company Finance Director STP For $1.2 Million Mail Fraud Scheme / Used Funds To Pay For Personal Expenses

- Employee For Chocolate Company STP For Stealing 19,000 Trade Secrets Including Recipes & Marketing Strategies

- JPMorgan Claims Former Employee Stole Trade Secrets To Solicit Former Clients At His New Job

- And Many More….

INSIDER THREAT INCIDENTS REPORT FOR FEBRUARY 2026

EXAMPLES FROM REPORT / (STP = Sentenced To Prison)

- Research Survey Of 500+ IT College Students Finds 60% Said They Would Leak Information In Exchange For Kickbacks
- 2 U.S Postal Service Employees Charged For Roles In $63 Million Stolen Check Scheme
- Social Security Administration Employee STP For Role In Embezzling $3 Million+ Using Fraudulent Benefits Applications
- General Services Administration Contracting Officer Pleads Guilty To Receiving $100,000+ In Bribes & Sports Car For Awarding Contracts
- DC Government Employee Pleads Guilty To Stealing And Selling $30,000 Of Government Laptops
- Medical Diagnostics Company Sales Director STP For Role In $70 Million Medicare Fraud & Kickback Scheme
- Employee STP For Embezzling $8.5 Million+ From Employer / Used Funds To Purchase Porsche & Home
- Florida State Employee & 5 Others Arrested For $1.7 Million Property Damage Fraud Scheme
- Senior Manager For Large Retailer STP For Embezzling $1.9 Million Using Fraudulent Invoices & Shell Companies
- TD Bank Employee Pleads Guilty To Accepting $6,000+ In Bribes For $5.5 Million Money Laundering Scheme To Colombia
- 3 Silicon Valley Engineers Working For Google & Other Tech Companies Charged For Theft Of Trade Secrets
- And Many More...

INSIDER THREAT INCIDENTS REPORT FOR MARCH 2026

EXAMPLES FROM REPORT / (STP = Sentenced To Prison)

- Department Of Energy (DOE) Whistleblower Reveals Contracting Company Fraudulently Overcharged DOE $3.4 Million+
- U.S. Marine Corps Intelligence Analyst Charged With The Transmission Of SECRET Classified Information To Unauthorized Individuals
- U.S. Postal Employee STP For $364,000+ Bank Fraud Scheme Involving Stolen Mail
- Chief Financial Officer STP For Stealing $35 Million From Start-Up Tech Firm / 60 Employees Laid Off
- Bank CEO Pleads Guilty To $24 Million+ Wire Fraud Conspiracy Causing Bank To Collapse
- Medical Laboratory CEO & Employees Indicted In $24 Million+ Health Care Fraud Scheme
- Company Office Manager / Bookkeeper Charged With Embezzling $10 Million+ Over 4 Years / Used Funds For Personal Expenses
- Johnson & Johnson Suing Former Employee For Theft Of 7,000 Trade Secret Documents After Receiving A Negative Performance Review
- Data Analyst Contractor Stole Company Data & Extorted His Company For $2.5 Million After Finding Out His Contract Was Ending
- Healthcare Employee Admits To Accessing & Stealing 1.2 Million+ Patient Records After Being Terminated
- And Many More…….

INSIDER THREAT INCIDENTS REPORT FOR APRIL 2026

EXAMPLES FROM REPORT / (STP = Sentenced To Prison)

- Report States That Gen Z Workers Are Sabotaging AI Systems For Fear Of Job Replacement
- Disgruntled Employee Charged For Setting Fire To 1.2 Million Square Foot Warehouse Causing Approximately $500 Million In Damage
- U.S. Army Soldier Charged With Using Classified Information To Profit $409,000+ From Polymarket Prediction Betting Website
- U.S. Army Employee Charged With Leaking Top Secret Information To Journalist
- U.S. Air Force Master Sergeant Pleads Guilty To 9 Year $37 Million Contract Bid Rigging & Bribery Scheme That Defrauded USAF
- Tesla Suing Vendor For Stealing $1 BILLION In Trade Secrets
- Employee Pleads Guilty To Embezzling $26 Million+ From Employer With Help Of Boyfriend / Used Funds To Pay Off Vehicles, Living Expenses, Credit Cards, Etc.
- Employee STP For Embezzling $3.8 Million Over 8 Years Using Altered & Fake Invoices Causing Company Serious Harm
- 20 Year Employee Pleads Guilty To Embezzling $3.7 Million Use Various Fraud Schemes
- Company Account Manager STP For Embezzling $2.8 Million+ / Used Funds For Luxury Items, Credits Cars & Real Estate
- Chief Financial Officer STP $4.5 Million Fraud Scheme
- And Many More...

INSIDER THREAT INCIDENTS REPORT FOR MAY 2026

EXAMPLES FROM REPORT / (STP = Sentenced To Prison)

- Terminated Employee Pleads Guilty To Detonating Explosive Device Under Former Supervisor's Vehicle At His Residence
- Employees Are Using Artificial Intelligence To Produce Phonographic Images Of Children & Employees
- 4 Reports Reveal That Employees Are Selling Their Login Credentials To Hackers To Gain Access To Corporate Networks
- IT Contractor STP For Hacking Employer's Network In Retaliation For Termination / Caused $860,000+ In Damages
- University Hospital Pharmacist Charged For Installing Spyware & Unauthorized Access To Computers For 8 Years
- Former CIA Officer Arrested For Stealing 300 Gold Bars Worth $40 Million+ From CIA & Falsifying Background
- 2 U.S. Postal Service Employees Plead Guilty To Stealing $84 Million+ In U.S. Treasury Checks
- Financial Services Company Employee Charged For $6.6 Million Wire Fraud Scheme Over 9 Years / Used Funds To Make $3.2 Million Of Credit Cards Payments, Etc.
- Fuel Company Chief Financial Officer Charged With Embezzling $12 Million Over 8 Years / Used Funds For Gambling
- Hospital Employee Accused Of Stealing $2.5 Million Worth Of Medical Supplies
- DOJ Contractor Employee STP For Stealing Cell Phones Worth $1.3 Million & Selling Them/ Used Funds For Gambling, Vacations, SUV, Etc.
- And Many More....

INSIDER THREAT INCIDENTS REPORT FOR JUNE 2026

EXAMPLES FROM REPORT / (STP = Sentenced To Prison)

- Former National Security Advisor John Bolton Pleads Guilty To Retaining & Transmitting Classified Information
- U.S. Army Recruiter Pleads Guilty To Stealing PII Of U.S. Army Recruits For $266,00 Identity Theft Loan Scheme
- 3 School Employees STP For Embezzling Nearly $400,000 Of Federal Program Funds
- Mortgage Company Suing Competitors & 31 Former Employees For Stealing Trade Secrets
- Google Employee Charged With Making $1.2 Million+ By Trading Confidential Business Information On Polymarket Betting Platform For Profit
- City Employee Pleads Guilty To Helping Embezzle & Launder $1.5 Million Of City Funds / Used Funds To Pay Personal Credit Card, Wedding Reception, Etc.
- Bank Manager Charged With Embezzling $1.9 Million From Bank
- Union President, His Wife, Union Vice President & Union Treasurer Convicted For Embezzling $7 Million For 15+ Years / Used Funds For Lavish International Travel
- Hawaii County Housing Official STP For His Role In $11 Million+ Scheme To Receive Bribes From Businessman & Attorneys
- Bank Manager Charged With Embezzling $1.9 Million From Bank
- Bank Branch Manager STP For Embezzling $800,000+ / Used Funds Lost Engaging In Foreign Currency Trading
- And Many More…..

INSIDER THREAT INCIDENTS REPORT FOR JULY 2026

- White House Teleprompter Operator Accused Of Making $100,000 Online By Betting On President Trump's Speech
- Defense Contractor To Pay $7.75 Million For Employing Department of War Employee Who Was Also Working As A Contractor
- Company Senior Director Of Engineering STP For Using Company Credit To Purchase $4 Million Worth Of Apple Products Over 8 Years & Then Sold Them
- 2 TD Bank Employees STP For $92 Million Money Laundering Scheme & Accepting Bribes
- Bank Chief Financial Officer STP For $4.3 Million+ Bank Loan Fraud Scheme
- Company Accounting Manager Pleads Guilty To Embezzling $3.2 Million+ / Used Funds For Gambling, Student Loan Debt, Etc.
- Chief Financial Officer Pleads Guilty To Laundering $67 Million Of Organizations Funds
- Company Financial Controller Pleads Guilty To Embezzling $1 Million+ / Used Funds To Purchase Ford F-150 Pickup Truck
- Employee Sentenced STP For Embezzling $385,000+ From Her Employer Causing Severe Impacts / Used Funds To Pay Husband & Personal Expenses
- 8 Individuals Including Current & Former NYC Correction Officers, Texas Parole Officer, & NYC Transit Authority Employee Charged In $3 Million+ Check Fraud Scheme
- And Many More...

INSIDER THREAT INCIDENTS REPORT FOR AUGUST 2026

- FBI Supervisor Confesses To Stealing Nearly $1 Million In Crypto Belonging To Suspect FBI Was Investigating
- U.S. Customs Border & Protection Officer STP For Accepting Multiple $10,000 Bribes To Allow Drugs To Enter The U.S. Through Their Inspection Lanes / Used Funds For Luxury Lifestyle
- Maryland National Guard Member Pleads Guilty To $2.2 Million+ Money Laundering Scheme
- Operations Manager Of Wholesale Drug Distributor STP For Role In Scheme To Buy $47 Million+ In Prescription Medications & Resell For Profit
- Employee STP For Embezzling $26 Million+ From Employer With Help Of Boyfriend / Used Fund To Live In Mansions, Drive Luxury Cars, Etc.
- Data Analyst STP For Extorting Employer For $2.5 Million / Threatened To Release Sensitive Data When He Found Out That His Contract Was Not Being Renewed
- Law Firm Paralegal Guilty Of Embezzling $1.8 Million+ Over 6 Years / Used Funds To Purchase 2 Homes
- Executive Director In Goldman Sachs Investment Banking Division Convicted For Paying $1 Million+ In Bribes To Ghanaian Government Officials
- Williams-Sonoma Executive Pleads Guilty To $16 Million Kickback, Fraud & Money Laundering Scheme
- Nike Employee Charged For Role In Running $1 Million Kickback Scheme Against Company
- Company Financial Manager STP For $18 Million Loan Fraud Scheme In Collusion With Sister & Brother in Law
- Philips Medical Systems Engineer Convicted For Stealing Trade Secrets On Behalf Of Chinese Competitor
- And Many More…

VERY DAMAGING INSIDER THREAT INCIDENTS

EXAMPLES (Sentenced To Prison (STP)

LOST JOBS / COMPANY GOES OUT OF BUSINESS

- Bank President STP For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations
- Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs
- Controller Of Oil & Gas Company Sentenced To Prison For $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs
- Credit Union CEO STP For Involvement In Fraud Scheme That Resulted In $10 Million In Losses, Forcing Credit Union To Close
- 2 Former Credit Union Employees (Sisters) Sentenced To Prison For Embezzling $1.5 Million Over 6 Years - Forcing Credit Union Out Of Business
- And Many More…

VERY DAMAGING FINANCIAL IMPACTS

- Financial Trader Facing Criminal Charge For Stealing Source Code Worth $1 BILLION To Build His Own Company
- Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION
- Goldman Sachs (GS) Managing Director STP For Role In $1.6 BILLION+ Bribery & Money Laundering Scheme / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty
- Wells Fargo Executive Pleads Guilty To Opening Millions Of Accounts Without Customer Authorization - Wells Fargo Agrees To Pay $3 BILLION Penalty
- CEO, Vice President Of Business Development And 78 Individuals Charged In $2.5 BILLION In Health Care Fraud Scheme
- Former Metallurgist Lab Director Sentenced To Prison To Falsifying Test Results For Strength Of U.S. Navy Submarines Hulls / Navy Has Spent $14 Million To Ensure Submarines Are
- And Many More…

SABOTAGE OF WORKPLACE

- Chicago Airport Contractor Employee Sets Fire To FAA Telecommunications Infrastructure System
- IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+
- School IT Department Employee Sentenced To Prison For Computer Sabotage After Termination / Download 300+ Usernames & Passwords Before Termination
- IT Contractor Sentenced To Prison For Hacking Employer's Network In Retaliation For Termination / Caused $860,000+ In Damages
- Company Software Developer Sentenced To Prison For Sabotaging Network After Being Placed On Leave / Impacting 1000+ Employee Globally
- Disgruntled IT Worker Sentenced To Prison For Attack Against Employer After Being Suspended From Work / Caused $270,00+ In Damages
- And Many More…

WORKPLACE VIOLENCE

- Amazon Employee Charged With Murder Of Co-Worker
- Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee
- Veterans Affairs Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences For Murdering 7 Veterans
- Former FedEx Employee That Killed 8 People Had Mental Health Problems
- Xerox Employee Receives Life In Prison For Credit Union Robbery And Murder
- Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants

- Disgruntled Employee Charged For Setting Fire To 1.2 Million Square Foot Warehouse Causing Approximately $500 Million In Damages
- School Bus Driver Sentenced To Prison For Setting Bus On Fire That Had 42 Children
- Terminated Employee Pleads Guilty To Detonating Explosive Device Under Former Supervisor's Vehicle At His Residence
- Disgruntled Athletic Club Employee Drove Car Packed With Explosives That Detonated Into Club & Dies
- And Many More…

INSIDER THREAT AWARNESS VIDEOS

Education, awareness and reporting are critical for Insider Risk Management and Insider Risk Management Programs. Creating a culture of See Something, Say Something is necessary to report employee risks and threats, before they could seriously impact an organization.

FBI Movie: Betrayed

Doug Collins has been a highly-respected analyst at the FBI for twenty-five years. He is liked and admired by all the members of his team, but they've seen changes in Doug recently: an attractive young girlfriend, working odd hours, increased frustration at work. And then there was the time he was seen texting on his Blackberry from inside the SCIF. It's all probably nothing. They know his recent divorce has been tough on him. It's not like he's a spy. But what if he is? What is the price of silence? (Watch Video)

FBI Movie: The Company Man

As part of a nationwide campaign to raise awareness of the growing economic espionage threat, the FBI has released a short video, "The Company Man: Protecting America's Secrets." Based on an actual case, the video illustrates how one company was targeted by foreign actors and what the FBI did to help. (Watch Video)

FBI Movie: Game Of Pawns

Glenn Shriver is an American convicted of conspiracy to commit espionage for China. At the behest of Chinese Intelligence Officer, Shriver unsuccessfully applied for jobs with the US State Department and CIA, meeting with handlers from China more than 20 times. (Watch Video)

FBI Movie: The Nevernight Connection

This FBI and National Counterintelligence and Security Center film—inspired by the case of former CIA officer Kevin Mallory—details the fictional account of a former U.S. Intelligence Community official who was targeted by China via a fake profile on a professional networking site and recruited to turn over classified information before being arrested. The FBI and NCSC seek to raise awareness of this issue and help individuals in the private sector, academic and research communities, and other U.S. government agencies guard against this threat posed by foreign intelligence services. (Watch Video)

National Insider Threat Task Force - Any Given Day Insider Threat Awareness Video
Life stressors impact us all – at work and at home. Watch how one employee struggles to deal with his stressors…and how a co-worker responds to a potential insider threat. (Watch Video)

DHS Understanding Insider Threat Awareness Video
The Understanding the Insider Threat video uses security and behavior experts to discuss how insider threats manifest in a variety of ways including terrorism, workplace violence, and breaches of cybersecurity. Understanding how to recognize and respond to these various types of insider threats, whether non-violent or violent, increases an organization's ability to protect both its people and sensitive information.
(Watch Video)

DHS Insider Threat Awareness Video
Watch Video

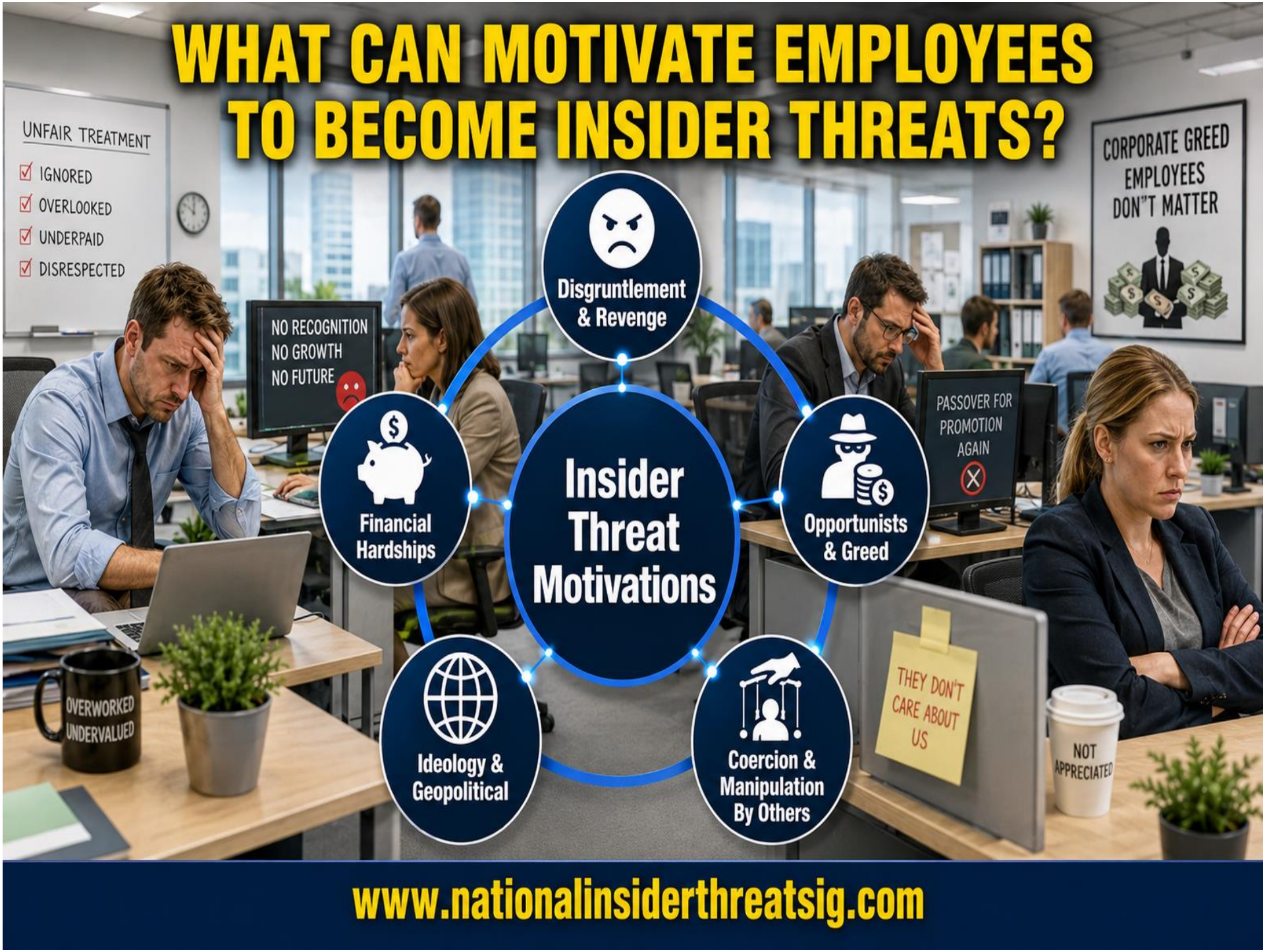
Defense Counterintelligence & Security Agency Insider Threat Awareness Training Video
Watch Video

Defense Counterintelligence & Security Agency For Insider Threat for Senior Leaders
Watch Video

Department Of The Navy Insider Threat Awareness Video
Watch Video

Department Of Energy Insider Threat Awareness Video
Watch Video

Terminal Risk Videos / Counterintelligence & Security Threats
These 10 videos were jointly produced by NCSC, NSA, FBI and State Department and focus on the Counterintelligence and security threats faced by the private sector at home and abroad. They reflect real-life threats faced by the U.S. private sector from terrorists, foreign intelligence services and foreign competitors. (Watch Videos)


WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?
UNFAIR TREATMENT
IGNORED
OVERLOOKED
UNDERPAID
DISRESPECTED
NO RECOGNITION
NO GROWTH
NO FUTURE
CORPORATE GREED EMPLOYEES DON"T MATTER
PASSOVER FOR PROMOTION AGAIN
Disgruntlement & Revenge
Financial Hardships
Insider Threat Motivations
Opportunists & Greed
Ideology & Geopolitical
Coercion & Manipulation By Others
OVERWORKED UNDERVALUED
THEY DON'T CARE ABOUT US
NOT APPRECIATED
www.nationalinsiderthreatsig.com

WHY DOES AN ORGANIZATION NEED AN INSIDER RISK MANAGEMENT PROGRAM (IRMP)?

An IRMP will protect an organizations assets and work in a **PROACTIVE** manner to identify employees who may pose a risk or threat to the organizations assets, to prevent any negative impacts to the organization.

Unfortunately because of inaccurate information some employees may have received, they may think an IRMP is a witch hunt targeting employees. **This is NOT TRUE**. An IRMP will protect employees from the possibility of them loosing their jobs, large layoffs or the company going out of business.

Very damaging Insider Threat incidents related to financial fraud could be occurring within a government agency or company on a daily basis, and may sometimes go undetected for 5-10 years or more. This makes the resulting damages much more severe when the fraud is detected.

After reviewing this report, and seeing the **EYE OPENING** damages and impacts that disgruntled or opportunist can cause, the NITSIG hopes employees have a much more comprehensive understanding of why an IRMP is needed to protect an organization assets.

Because of the severe financial damages and other operational impacts that can be caused by **JUST 1 EMPLOYEE** or employees in collusion with other employees, or external individuals, organizations must make Insider Threat Awareness more than just a 1 once a year briefing.

Many organizations use the NITSIG monthly Insider Threat Incidents Reports as an awareness tool to educate employees on the importance of reporting employees, who's behavioral indicators raise concern, or their intent or actions could cause harm to the organizations assets: Facilities, Financial Assets, Employees, Data, Computer Systems and Networks.

Joining The NITSIG Is FREE

To join the NITSIG you must complete and sign the membership application. Instructions for e-mailing the application to the NITSIG are in the application. Once the NITSIG receives your application, it will be reviewed for approval. You will receive an e-mail once your application has been approved.

Contact Information

If you have any questions regarding the Insider Threat Awareness Briefing, please contact:

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org
561-809-6800

CEO Insider Threat Defense Group, Inc.
Insider Risk Management Program Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com